Context-Aware Authorization and Anonymous Authentication in Wireless Body Area Networks

Amel Arfaoui, Ali Kribèche, Omar Rafik Merad Boudia, Asma Ben Letaifa, Sidi-Mohammed Senouci, Mohamed Hamdi

Context-Aware Authorization and Anonymous Authentication in Wireless Body Area Networks

Amel Arfaoui*ǂ, Ali Kribecheǂ, Omar Rafik Merad Boudiaǀ, Asma Ben Letaifa†, Sidi Mohammed Senouciǂ, Mohamed Hamdi*
*Digital Security Unit, SupCom University of Carthage, Tunisia
ǂDRIVE EA1859, Univ. Bourgogne Franche Comté, France
ǀComputer Science Department, University of Oran 1 Ahmed Ben Bella, Algeria
†MEDIATRON Lab., Sup'Com, University of Carthage, Tunis, Tunisia
{amel.arfaoui, Sidi-Mohammed.Senouci, Ali.Kribeche01}@u-bourgogne.fr, rafik.merad@univ-oran.dz, {mmh, asma.benletaifa}@supcom.tn

***Abstract*—With the pervasiveness of the Internet of Things (IoT) and the rapid progress of wireless communications, Wireless Body Area Networks (WBANs) have attracted significant interest from the research community in recent years. As a promising networking paradigm, it is adopted to improve the healthcare services and create a highly reliable ubiquitous healthcare system. However, the flourish of WBANs still faces many challenges related to security and privacy preserving. In such pervasive environment where the context conditions dynamically and frequently change, context-aware solutions are needed to satisfy the users' changing needs. Therefore, it is essential to design an adaptive access control scheme that can simultaneously authorize and authenticate users while considering the dynamic context changes. In this paper, we propose a context-aware access control and anonymous authentication approach based on a secure and efficient Hybrid Certificateless Signcryption (H-CLSC) scheme. The proposed scheme combines the merits of Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) and Identity-Based Broadcast Signcryption (IBBSC) in order to satisfy the security requirements and provide an adaptive contextual privacy. From a security perspective, it achieves confidentiality, integrity, anonymity, context-aware privacy, public verifiability, and ciphertext authenticity. Moreover, the key escrow and public key certificate problems are solved through this mechanism. Performance analysis demonstrates the efficiency and the effectiveness of the proposed scheme compared to benchmark schemes in terms of functional security, storage, communication and computational cost.**

Keywords— IoT; WBAN; Context-aware security; Anonymous Authentication; Signcryption.

I. INTRODUCTION

In recent years, the rapid technological advancements in innovative health-oriented networking, wireless communication technologies and medical sensors have enabled the Wireless Body Area Network (WBAN) to become a promising networking paradigm [1][2]. Many technologies have proved their efficiency in supporting WBAN applications, such as remote monitoring, biofeedback and assisted living. A WBAN consists of a set of implantable medical devices (IMDs) [3] collecting real-time biomedical data such as heart rate, blood pressure, and pulse. Based on this data, healthcare providers could assess the patient's status and provide the appropriate clinical diagnosis. The collected data is delivered to the medical staff through a data sink. The data sink may be a smartphone that has the ability to communicate with a remote medical server through cellular networks or the Internet. In this context, the deployment of WBAN provides ubiquitous healthcare system that ensures timely medical treatment and clinical diagnosis.

Unlike conventional sensor networks, a WBAN deals with more critical and sensitive patient information that imposes several privacy preserving, security and safety concerns. Therefore, the collected data should be handled, transmitted, and analyzed only by authorized users in order to get correct and accurate treatments. Since the patient's information is transmitted through an open channel, it can be eavesdropped, intercepted and modified. In this context, counterfeited health-related data may mislead the medical staff to make the appropriate decision, which may convolute the patient's situation. Furthermore, the dynamic and heterogeneous WBAN environment imposes more challenges for the design of security and access control mechanisms. In fact, authentication and authorization should be adapted to the context changes (such as patient's condition, data consumers' roles, security domain...) in order to make the right decision on the right time by the right party. For example, a nurse who has a restricted access compared with a doctor in normal situations can gain additional permissions in emergency situations. In such critical context, privacy may be restricted or relaxed given that safety is more important than security. In fact, after detecting a critical situation an alarm is sent to the direct doctor. If he doesn't response during a predefined period, the privacy can be restricted and the nurse can access to patient's data.

In order to address the above issues, we propose a context-aware authentication and access control approach to adaptively adjust the security and privacy level according to the current situation. We introduce a novel Hybrid Certificateless Signcryption (H-CLSC) scheme that combines the Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) and Identity-Based Broadcast Signcryption (IBBSC) features [4][5] to address the secure communication problem and provide an adaptive context-aware privacy. A WBAN client in a normal situation can define the access control policy to his own data. For example, by constructing the access structure ({status= normal}AND {hospital A} AND {Vascular Surgery}), the data requires that on normal situations only doctors from the Vascular Surgery Center in hospital A can have the access right. The major contributions can be summarized as follows.

- A novel context-aware authentication and access control approach that provides a dynamic authorization to the patient's data based on the contextual information
- A Hybrid Certificateless Signcryption (H-CLSC) scheme with public verifiability and ciphertext authenticity in which the validity of the ciphertext can be verified without decryption.
- An anonymous signcryption mechanism for privacy preserving and fine-grained access control that merges the worthiness of CP-ABSC and IBBSC.
- Resilience against the key escrow problem and impersonation attack by the Key Generator Center (KGC). Given that the KGC can generate only user's partial private key, it can't decrypt messages or impersonate users.

The remainder of the paper is organized as follows. Section II presents an overview on security and privacy in WBAN. A mathematical background is introduced in section III. The system model and the design goals in terms of security and privacy requirements are described in Section IV. An efficient H-CLSC scheme for authentication and access control is given in Section V, followed by the performance analysis in Section VI. Finally, a conclusion is drawn in Section VII.

II. Related Work

Recently, the privacy preserving and anonymous authentication which seem as conflicting goals have attracted an extensive attention from both the research community and industry. In this context, many authentication and access control schemes for WBANs have been proposed. For instance, in [6], Liu et al. used the bilinear pairing defined on the elliptic curve to design a new anonymous authentication scheme based on certificateless signature. A user should be authenticated before accessing the patient's health information stored in network server. The proposed model can avoid both public key certificates and key escrow problem. However, [7] found that Liu et al. scheme suffers from impersonation attack. Therefore, they provided an improved anonymous authentication scheme to address the aforementioned security problem. In [8], the authors proposed an efficient certificateless signcryption model for access control in wireless body area networks. In the registration phase, every user first generates a public key pair, and sends it to the Key Generator Center (KGC) in order to get a partial private key. Upon receiving his partial private key, the user could compute his full public key pair. As only registered user could generate this public key pair, this generation can be considered as a measure to verify the legitimacy of the user. Given that only the public key is transferred, the user's identity is hidden and anonymity is ensured. However, in their scheme they consider that all the data consumers have the same privileges. In [9] an efficient and certificateless scheme that exploited the generalized signcryption (CLGSC) model was proposed. The security analysis demonstrated that the adopted scheme can achieve data confidentiality and integrity, mutual authentication, unlinkability and anonymity. From the performance perspective, it has been proved that it can outperform the existing schemes in terms of computational and communication overhead. In [10], a remote anonymous authentication protocol with revocability for extra-body communication in WBANs has been proposed. However, it involved large amounts of computation and energy consumption.

In order to achieve privacy preserving and fine-grained access control, Attribute Based Cryptography (ABC) is considered as a promising approach that can provide a lightweight and adaptive access control. In such scheme, each user is associated with a set of attributes and data is encrypted according to an access structure. Only receivers whose attributes satisfy the access policy can decrypt the ciphertext. A Ciphertext-Policy Attribute Based Encryption (CP-ABE) scheme was proposed in [11] in order to secure the data communications between sensor nodes and the data sink/data consumers. In fact, it considers a role-based access control by employing an access control tree constructed from the attributes of the data. However, it suffers from key escrow problem and high computational cost.

Most of the previous works don't involve the contextual information for the access control and authentication. Therefore, we should deal with the following critical technical challenge when designing a WBAN security mechanism: how to properly regulate and adjust the access rights and authentication policy of the different data consumers while considering the dynamic context changes?

III. Preliminaries

In this section, we introduce some preliminary knowledge regarding the notations, the background information on Bilinear Pairings and the cryptographic primitives used in this paper.

A. Notations

Notation	Description
q	A large prime number
$\mathbb{G}_1$	An additive group with order q
$\mathbb{G}_2$	A multiplicative group with order q
e	A bilinear pairing
P	A generator of the group $\mathbb{G}_1$
$H_1\ H_2\ H_3$ $H_4\ H_5$	One-way hash functions
PK, MK	System public key and master key
PK_{Ui}	The public key of user i
SK_{Ui}	The secret key of user i
U	The universe of attributes
U_i	The attributes set of user i
A	An access structure
C	The contextual information {user's domain, data type, patient's status}
t_s	The current timestamp of the signer
$E_k()$, $D_k()$	The symmetric encryption and decryption where k is the key.

Table 1. Variables and their descriptions

B. Bilinear Pairings

Let $\mathbb{G}_1$ be a cyclic additive group of prime order q and $\mathbb{G}_2$ be a cyclic multiplicative group of the same order q. A bilinear pairing is a map e: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and satisfies the following properties:

- Bilinear: A map e: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is bilinear if and only if for two random points P, $Q \in \mathbb{G}1$ and two random elements a, $b \in \mathbb{Z}q$, we have e $(aP, bQ) = e\ (P, Q)^{ab}$
- Non-degeneracy: $\exists P, Q \in \mathbb{G}_1$ where $e\ (P, Q) \neq 1\mathbb{G}_2$
- Computability: $\forall\ P, Q \in \mathbb{G}_1$, there is an efficient algorithm to compute $e\ (P, Q)$ in polynomial time.

It is well known that there is no algorithm that could solve the following problems in polynomial time:

- *Computational Diffie–Hellman(CDH) problem*: given $P, aP, bP \in \mathbb{G}_1, \forall\ a, b \in \mathbb{Z}q$, it is infeasible to compute abP in polynomial time.
- *DBDH (Decision Bilinear Diffie-Hellman) problem*: Given two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with the same prime order q, a bilinear map e: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and a generator P of $\mathbb{G}_1$, the objective of DBDH is to compute $e\ (P, P)^{abc}$ in $(\mathbb{G}_1, \mathbb{G}_2, e)$ from the given $(P, aP, bP, cP), \forall a, b, c \in \mathbb{Z}q$.

C. Definitions

1) Ciphertext-Policy Attribute-Based signcryption (CP-ABSC): it includes the following four algorithms

- Setup(1^{λ}): Given a security parameter λ, the KGC generates a master secret key MK that is kept private and a public key PK shared by users.
- KeyGen (PK, MK, U): The KGC takes the master secret key MK, the attribute set of the user U, and the public key of the system PK as inputs. It outputs the private key SK_U.
- Signcryption (PK, M, SK_{Us}, $\mathcal{A}$): The signer takes the public parameters PK, a plaintext M, a signing private key SK_{Us} and an access structure $\mathcal{A}$ as inputs. The algorithm will signcrypt M and generate a ciphertext CT such that only a user who possesses a set of attributes that satisfy the access policy will be able to designcrypt.
- Designcryption (CT, PK, SK_{Ud}): The receiver takes as input the ciphertext CT, the public parameters PK and his decryption key SK_{Ud}. The algorithm outputs a message M or a reject symbol $\perp$.

2) Identity- Based Broadcast signcryption (IBBSC): The IBBSC scheme consists of four algorithms as follows:

- Setup(1^{λ}): The KGC takes a security parameter λ as an input. Then it outputs a master secret key MK and a public key PK.
- KeyGen (PK, MK, ID): The KGC takes the master secret key MK, the identity $ID \in \{0, 1\}^{\lambda}$, and the public key of the system PK as inputs. It outputs the private key SK_{ID}.
- Signcryption (PK, M, S, SK_{IDs}): The signcryption algorithm is executed by the sender which takes the public parameters PK, the signing key SK_{IDs}, a plaintext M, and a set of identities $S = \{ID_1, ...ID_n\}$ of receivers as inputs. It encrypts the plaintext M to generate the ciphertext CT.
- Designcryption (CT, PK, SK_{IDd}): The receiver takes as input the ciphertext CT, the public parameters PK and the decryption key SK_{IDd}. The algorithm outputs a message M or a reject symbol $\perp$.

3) Conversion between access structures DNF and a set of identities

In our scheme, we will exploit the conversion between an IBBSC and a CP-ABSC that supports Boolean functions in DNF [4][5]. For such scheme, an access structure $\mathcal{A}$ can be uniquely related to an identity ID_A, whose length equals to $|U|$, i.e. the size of the universe U of attributes. Specifically, for an access structure $\mathcal{A}$, for $i = 1$ to $|U|$, if an attribute X_i is in $\mathcal{A}$, then set the i^{th} bit of ID_A as 1; otherwise set it as 0. For instance, if $U = \{A, B, C, D, E\}$ and $\mathcal{A} = A$ AND B AND $C = \{A, B, C\}$, then we can construct the identity as $ID_A = 11100$. An access structure can be represented as a disjunction of conjunctive clauses, i. e. disjunctive normal form (DNF). Since every clause in a DNF formula contains only AND gates, it can be converted to an identity. Therefore, a DNF structure implies a set of identities $S = \{ID_1, ...ID_n\}$, which can be considered as the receivers set in an IBBSC scheme.

IV. Model and Design Goals

A. System Model

We consider a WBAN communication system presented in Fig.1. It mainly consists of three entities: Key Generator Center (KGC), the WBAN client and a data consumer (such as a nurse, a doctor, an insurance company a physician, family member, friend…).

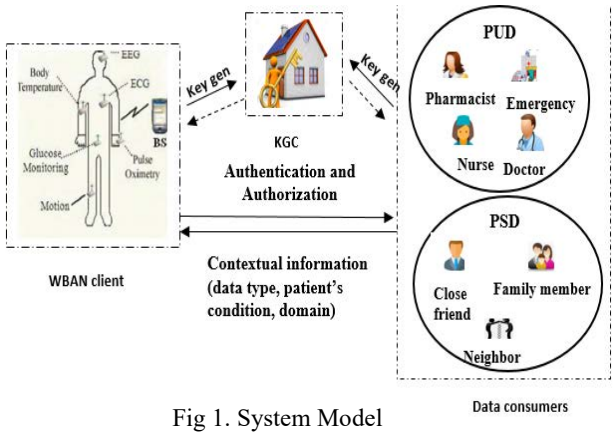

Fig 1. System Model

The different functions of each entity are presented as follows:

- The Key Generator Center(KGC) is responsible for system initialization, public parameters generation and users' secret keys assignment. A data consumer should prove his legitimacy to the KGC which will generate his secret key. In order to prevent collusion attacks, user's private keys are randomized. Upon receiving the public parameters, the WBAN client can construct his access structure and signcrypt his data on the basis of a signing policy. Once the data consumer's attributes satisfy the

access structure, he can decrypt the message using his secret key.

- WBAN Client consists of some sensor nodes and a controller which is used to store the patient's data in an encrypted form. When a data consumer wants to access to a data item from the WBAN client in a given contextual information, he can verify the validity of the ciphertext and decrypt the data as long as he possesses the decryption attributes set specified by the signing access structure.
- Data Consumers refer to the users coming from two different domains, namely public domain (PUD) and personal domain (PSD) [12]. Data consumers in PUD include healthcare providers e.g., doctors, physicians, nurses, and researchers. However, users who come from the PSD are personally associated with the WBAN client (such as family members or close friends). To decrypt a message, data consumers need not only to have the attributes that satisfy the access structure specified by the data owner but also to determine the contextual information related to their domain, the patient's condition severity (normal, serious or emergency), and data type (sensitive, non-sensitive). For instance, in emergency situations the access to the requested data should be granted on time. Upon receiving the information doctors react immediately in order to prevent more critical situations that can affect the patient's life. Thus, higher priority is assigned to the patients' safety than to the privacy preserving.

B. Security Requirements

The dynamic WBAN environment and the wireless communication between the data owner and the data consumer make the authentication and the patient's privacy vulnerable to many attacks. To guarantee secure communication in WBAN, a dynamic authentication scheme should be designed to support the following security requirements. These requirements involve not only security but also context-aware privacy. According to previous works [13][8][14] and the above analysis, the authentication scheme in WBAN should satisfy the following functionality features and security requirements.

- *Ciphertext Authenticity and public verifiability*: To ensure only authorized users could access to medical data and query messages be protected. It is necessary to provide a ciphertext authenticity and public verifiability where the validity and the origin of the ciphertext can be verified without knowing the content of the message or the receiver's private key.
- *Context-aware privacy*: Based on the contextual information (patient's condition, the user's role, the data type…), the authentication policy and the access structure are defined.
- *Anonymity*: To protect the patient's privacy, it is essential to ensure that no one including the data consumer and the KGC could obtain the patient's identity from the intercepted message.
- *Non-traceability*: Only anonymity is insufficient for privacy preserving. Therefore, it is necessary that the authentication scheme could guarantee non-traceability i.e. adversaries, unauthorized data consumers and KGC are not able to trace the WBAN client's action.
- *Resilience against attacks*: Due to the dynamic and open structure of WBAN, the access control and authentication for WBAN are susceptible to many attacks such as unauthorized access, the impersonation attack, the replay attack and the modification attack. Therefore, the authentication and authorization scheme should avoid those aforementioned attacks.

V. Efficient Hybrid Certificateless Signcryption (H-CLSC) Scheme

In this section, we exploit the transformation between CP-ABSC and IBBSC [4][5] which considers an access structure as a set of identities. The signer who possesses his own signing key can sign a message if his signing attribute set (corresponding to an identity ID_s) satisfies the signing policy. Based on the contextual information (patient's condition, the data sensitivity, data consumers' domain) and the set of decryption attributes (corresponding to an identity ID_d), only the receiver whose attribute set verifies the access structure can decrypt the ciphertext [15][16].

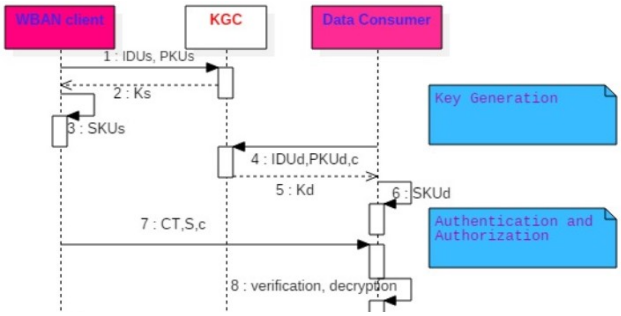

Fig 2. H-CLSC Authentication and Authorization scheme

The proposed H-CLSC scheme (presented in Fig 2) is composed by four algorithms. **Algorithm 1** describes the system initialization executed by KGC. Specifically, the KGC generates and distributes the public parameters to all the entities in the system. **Algorithm 2** presents the interaction between the WBAN client/data consumer and the KGC. Based on the contextual information c and the set of attributes owned by the user, he proves his authorization and permissions to the KGC. After verifying the authorization, the KGC uses the master key MK, the public parameters PK and the given attributes set U to generate a private key SK_U. In our scheme, we employ two kinds of key generation algorithms: *sExtract* that generates the signing key SK_{Us} and *dExtract* which set up the decryption key as SK_{Ud}. The Signcryption procedure is defined in **Algorithm 3** which is performed by the signer who defines an access structure $\mathcal{A}$ for a given contextual information c that includes the domain label, the data type as well as the patient's condition.

Algorithm 4 implements the Desyndecryption process, which is executed by the data consumer.

Algorithm 1 System Initialization

Input: 1^{λ}, the length of the plaintext $|M|$, a random integer w

Output: MK, PK

1. Select a prime q, a generator P of $\mathbb{G}_1$, and a bilinear map e: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
2. Choose five secure hash functions H_1: $\{0,1\}^* \rightarrow \mathbb{G}_1$ H_2: $\mathbb{G}_2 \rightarrow \mathbb{Z}_q^*$, H_3: $\{0,1\}^{|M|} \times \mathbb{Z}_q^* \times \cdots \times \mathbb{Z}_q^* \times \mathbb{G}_1 \rightarrow \mathbb{G}_1$, H_4: $\mathbb{Z}_q^* \rightarrow \{0,1\}^w$ and H_5: $\{0,1\}^w \rightarrow \{0,1\}^{|M|}$
3. Select a master key $MK \in \mathbb{Z}_q^*$ which is kept secret
4. Compute the corresponding public key $P_{pub} = MKP$
5. Publish the public parameters of the system
$$PK = \{\mathbb{G}_1, \mathbb{G}_2, q, e, P, P_{pub}, H_1, H_2, H_3, H_4, H_5\}$$

Algorithm 2 Key Generation (*sExtract*)

Input: the public parameters PK, the master key MK, the signing attributes U_s

Output: SK_{Us}

1. A signer with a set of signing attribute set U_s that is converted on an identity ID_{Us} generates a random number α_s
2. Calculate the public key $PK_{Us} = \alpha_s P$
3. Send $\{ID_{Us}\}$ to the KGC
4. The KGC computes $Q_s = H_1(ID_{Us})$ and $K_s = MKQ_s$
5. The KGC sends back $\{K_s\}$ through a secure channel to the signer
6. The signer calculates $h = H_1(PK_{Us}||ID_{Us})$ and his *own* signing key $SK_{Us} = K_s + \alpha_s h$

Algorithm 2 Key Generation (*dExtract*)

Input: the public parameters PK, the master key MK, the decryption attribute set U_d, the contextual information c

Output: SK_{Ud}

1. A data consumer with a set of attribute U_d that is converted to an identity ID_{Ud} selects a random number α_d
2. Calculate $PK_{Ud} = \alpha_d P$
3. Send (ID_{Ud}, c) to the KGC
4. The KGC calculates $Q_d = H_1(ID_{Ud})$ and $K_d = MKQ_d$
5. the KGC sends through a secure channel $\{K_d\}$ back to the data consumer
6. The receiver computes $h_2 = H_1(PK_{Ud}||ID_{Ud}||c)$ and defines his *own* decryption key $SK_{Ud} = K_d + \alpha_d h_2$

Algorithm 3 Signcryption

Input: An access structure $\mathcal{A}$, public parameters PK, a plaintext M, the signer private key SK_{Us} the contextual information c, the current timestamp t_s

Output: the ciphertext CT

1. The access structure $\mathcal{A}$ is converted to a set of n receivers with identities $S = \{ID_1, ...ID_n\}$
2. Choose a random number r and a bit string $\delta \in \{0,1\}^w$
3. Calculate $Y_i = rQ_{di}$, $U = rP$, $R_i = rh_{2i}$ where $Q_{di} = H_1(ID_i)$, $h_{2i} = H_1(PK_{Udi}||ID_i|c)$
4. For $i=1,2...n$, the signer computes $z_i = H_2(e(PK_{Udi}, R_i)\, e(P_{pub}, Y_i))$
5. Select randomly positive integer $s \in \mathbb{Z}_q^*$ and define a polynomial $f(x)$ with degree n as follows:
$$f(x) = \prod_{i=1}^{n}(x - z_i) + s(mod q) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$
6. Compute $\vartheta = \delta \oplus H_4(s)$, $Z = E_{H5(\delta)}(M)$, $X = e(Q_s, U)$ and $L = H_3(X, U, Z, \vartheta, c, t_s, a_0, a_1, \ldots a_{n-1})$
7. Calculate $V = rQ_S + LSK_U$
8. Generate the ciphertext $CT = < U, Z, \vartheta, V, t_s, a_0, a_1, \ldots a_{n-1} >$

Algorithm 4 Designcryption

Input: the ciphertext CT, the public parameters PK and the receiver's private key SK_{Ud}

Output: the plaintext M'

1. A receiver with an identity $ID_i \in S$ checks the validity of t_s while verifying $|t_s - \mathrm{t}| \leq \Delta t$ where Δt is the preset maximum transmission delay and t is the current time. Reject the message if it is not valid; otherwise
2. Compute $h = H_1(PK_{Us}||ID_{Us})$ and $Q_s = H_1(ID_{Us})$.
3. Compute $L = H_3(X, U, Z, \vartheta, c, t_s, a_0, a_1, \ldots a_{n-1})$
4. Verification: if the equation $X = (e(h, PK_{Us}) * e(Q_s, P_{pub}))^{-L} e(V, P)$ holds, the ciphertext is valid. Otherwise, the ciphertext is rejected and the receiver drops the decryption process
5. Compute $z_i' = H_2(e(SK_{Udi}, U))$ and $s = f(z_i')$
6. Compute $\delta = \vartheta \oplus H_4(s)$
7. Recover the message: $M' = D_{H5(\delta)}(Z)$

VI. Performance and Security Analysis of the H-CLSC scheme

In this section, we will evaluate the effectiveness of the proposed scheme through a security analysis. Then, a comparative study of benchmarking approaches will be presented to assess the security properties, the communication overhead, the storage overhead as well as the computation cost of the H-CLSC scheme.

A. Security Analysis

- *Confidentiality and Unforgeability*: The IBBSC has been proved to satisfy confidentiality (i.e. indistinguishability against adaptive chosen ciphertext attack (IND-CCA)) and unforgeability (i.e. Strong unforgeability against adaptive chosen messages attack (SUF-CMA)) in [15] [16]. In addition, it has been demonstrated in [4] [5] that if an IBBSC scheme is secure, then the conversion from a CP-ABSC to an IBBSC is secure. Therefore, the confidentiality and unforgeability of our proposed H-CLSC scheme are ensured.

- *Ciphertext authenticity and Public verification*: In the proposed scheme, any third party can verify the validity of the ciphertext $CT = < U, Z, \vartheta, V, t_s, a_0, a_1, \ldots a_{n-1} >$ without any information about the message M or the private key of the receiver. In fact, for a given public parameters PK, a sender identity ID_{Us} (corresponding to the signer set of attributes U_s), a signer public key PK_{Us}, anyone can verify the signer's signature and compute

$h=H_1(PK_{Us}||ID_{Us})$, $Q_s=H_1(ID_{Us})$ and $e(V, P) = (e(h, PK_{Us}) * e(Q_s, P_{pub}))^L * e(Q_s, U)$. If the ciphertext isn't valid, the receiver can reject the ciphertext without decrypting it.

- *Context-aware privacy*: In our construction the signcryption process involves the contextual information to determine who can access to what and under which context. In fact, each access structure is defined while taking into account the dynamic context changes which includes the patient's condition severity, the data type, the data consumer roles and their domains(PUD/PSD) in order to provide the right authorization to the right party

- *Anonymity and untractability*: During our authentication and authorization process, the WBAN client can sign a message using a set of signing attributes satisfying a given signing policy. In such assumption, a signature reveals nothing about the identity of the signer beyond what is explicitly revealed by the attribute-based authentication policy. Under this notion, different signatures can't be identified as sent by the same WBAN and we can assume that the signer is an authorized user. Therefore, unauthorized data consumers and adversaries can't disclose who is the WBAN client or assign the multiple authentication sessions to the same patient.

- *Impersonation attack by KGC and escrow problem*: In our construction, the private keys of the WBAN client and data consumer are generated by themselves and they are not known by KGC. Thus, the KGC can't decrypt messages or impersonate the WBAN client/the data consumer.

- *Replay attack*: To resist the replay attack, the ciphertext includes the timestamp. Upon receiving the signcrypted message, the data consumer will check the freshness of the timestamp t_s before executing the other steps of the designcryption process. In this case, the data consumer could detect the replay attack easily.

- *Modification attack*: To detect any unauthorized modification of the patient's data, the WBAN client should sign the message according to a given access structure using his private key. When a data consumer receives the patient's information he could identify any modification by checking the validity of the signature without disclosing the exact identity of the signer.

B. Performance Analysis

In this section, we evaluate the security and performance characteristics of our proposed scheme through quantitative analysis. The proposed scheme is compared with those of LRSA [9], R-CLE/S [10], CP-ABE [11] in terms of security properties, storage overhead, communication overhead and the main computational cost. We should indicate that the four schemes use different methods to design the authentication and authorization model. In addition, we will only consider the communication between one sender and one receiver to conduct the comparison between the different schemes. Only the resource-constrained devices (controller/sensor nodes) are considered. In our evaluation, the bilinear e employs the Tate pairing. The elliptic curve is defined over F_p. The order q of $\mathbb{G}_1$ and $\mathbb{G}_2$ is a 20-byte prime. In order to ensure 80-bit security level, p should be a 64-byte prime if $\mathbb{G}_2$ is a q-order subgroup of the multiplicative group of the finite field F_{p2}^*. According to [11], we can set p to be 42.5 bytes in length for the finite field F_{p3}^*. The length of an element in group $\mathbb{G}_1$ is 1024 bits using an elliptic curve with 160 bits q. Based on the standard compression method [8] [17], the size of an element in group $\mathbb{G}_1$ can be compressed to 65 bytes.

1) Comparisons of security propreties

In this subsection, we provide a functional assessment of the proposed scheme while comparing the security properties of the H-CLSC model with the different benchmark schemes in Table 2. The effectiveness of the security and privacy preserving scheme is evaluated in terms of confidentiality, integrity, anonymity, ciphertext authenticity, public verification, context-aware privacy, certificateless, untraceability, key escrow resilience and resistance against attacks.

scheme	Conf	Int	Anon	Ciph.Auth	Pub.Ver	Context-privacy	No cert	Untra	No.Key esc	Attack resistance
[9]	+	+	+	-	-	-	+	+	+	-
[10]	+	+	+	-	-	-	+	+	+	-
[11]	+	+	+	-	-	-	-	+	-	-
H-CLSC	+	+	+	+	+	+	+	+	+	+

Table 2. Overall comparison of security properties

2) Storage overhead

The storage overhead is an expressive metric of any authentication scheme for WBANs because both the client and the data consumer should store the secret keys to achieve authentication. In our H-CLSC scheme, either the WBAN client or the data consumer needs to store $\{SK_{Ui}\}$, where SK_{Ui} is an element of $\mathbb{G}_1$. The user's storage overhead is 65 bytes. As shown in Table 3, the WBAN client in the proposed scheme requires less storage overhead than the other schemes [9] [10] [11].

Scheme	WBAN client's storage overhead
LRSA [9]	$\lvert\mathbb{G}_1\rvert+\lvert Z_q^*\rvert$=85 bytes
R-CLE/S [10]	$2*\lvert\mathbb{G}_1\rvert+\lvert Z_q^*\rvert$=150bytes
CP-ABE [11]	$N*\lvert\mathbb{G}_1\rvert+\lvert Z_q^*\rvert=65*N+20$ bytes
H-CLSC	$\lvert\mathbb{G}_1\rvert$=65 bytes

Table 3. Storage overhead comparisons

3) Communication overhead

The ciphertext needs to be stored in the controller and transmitted to the data consumers when requested. In this context, the communication overhead is mainly associated to the size of the ciphertext. In the proposed scheme, the ciphertext size dependent on the number of consumers. In this study, we will consider only one data consumer. The WBAN client needs to transmit: $2\lvert\mathbb{G}_1\rvert+\lvert Z_q^*\rvert+\lvert M\rvert+w$, where w is the bit length of a string and we assume that w=10bytes.

Scheme	Controller (bytes)	Sensor node(bytes)
LRSA [9]	$4\|\mathbb{G}_1\|+6\|Z_q^*\|+2\|ID\|+\|M\|=420$	-
R-CLE/S [10]	$\|\mathbb{G}_1\|+8*\|Z_q^*\|+\|M\|+\|ID\|=255$	-
CP-ABE [11]	$5\|\mathbb{G}_2\|+24=236.5$	$10\|\mathbb{G}_2\|+76=501$
H-CLSC	$2\|\mathbb{G}_1\|+\|Z_q^*\|+\|M\|+w=180$	-

Table 4. Communication overhead comparisons

4) Computation Cost

In this subsection, we compare the proposed H-CLSC scheme with the three other schemes in terms of computational overhead. As the operations on pairing, exponentiation and multiplication heavily influence the computational overhead, we only take into account these three operations. We denote T_E the time consumed for one exponentiation operation, T_M the time consumed for one scalar multiplication in $\mathbb{G}_1$, and T_P the time for one pairing operation.

In our proposed H-CLCS scheme, the signcryption process in WBAN client takes six multiplication operations in $\mathbb{G}_1$ and three pairing operations in $\mathbb{G}_2$. The computational cost for the H-CLCS scheme and the other authentication and authorization models are presented in Table 5. According to [9], to quantify the running time of the operations, the algorithms are implemented on an Intel PXA270 processor at 624 MHz installed on the Linux personal digital assistant. The running time of the different operation are $T_E = 53.85$ms, $T_M = 30.67$ms, and $T_P = 96.20$ms, respectively.

Scheme	Controller (ms)	Sensor node(ms)
LRSA [9]	$9T_M$=276.03	-
R-CLE/S [10]	$11T_E+T_P$=688.5	-
CP-ABE [11]	$5T_P$=481	$10T_P$=962
H-CLSC	$3T_P+6T_M$=472.62	-

Table 5. Computation cost comparisons

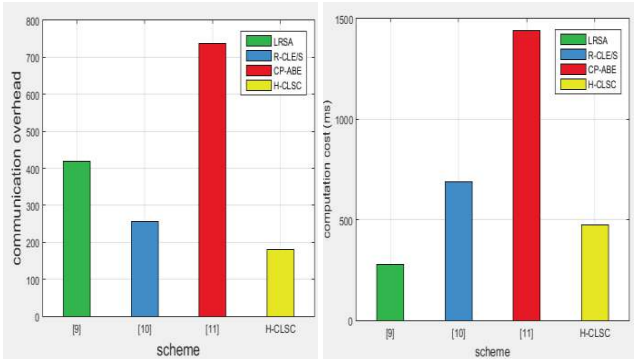

Fig 3. Communication and Computational cost comparisons

As shown in Fig 3, the proposed scheme is more efficient than the compared schemes in terms of communication overhead. However, it has the more computational cost compared to the LRSA scheme and achieves better performance compared to CP-ABE and R-CLE/S schemes.

VII. Conclusion and Future Work

In this paper, we addressed the problem of context-aware access control and authentication. For this purpose, we have proposed a novel efficient hybrid certificateless signcryption (H-CLSC) scheme with public verifiability and authenticity, which combines the CP-ABSC and IBBSC advantages in order to ensure not only context-aware privacy, anonymity and authentication but also to mitigate the key escrow problem. Performance analysis has proven the efficiency and effectiveness of the proposed model in terms of security, privacy level as well as the storage and communication cost. As future direction, we will give a formal security proof of the H-CLSC scheme and design a more efficient signcryption approach with less computational cost which will be more convenient for sensitive-delay WBAN applications.

REFERENCES

[1] T. Y. Wu and C. H. Lin, "Low-SAR path discovery by particle swarm optimization algorithm in wireless body area networks," IEEE Sensors J., vol. 15, no. 2, pp. 928–936, Feb. 2015.

[2] C. Yi, L. Wang, and Y. Li, "Energy efficient transmission approach for WBAN based on threshold distance," IEEE Sensors J., vol. 15, no. 9, pp. 5133–5141, Sep. 2015.

[3] D. Liu, Y. Geng, G. Liu, M. Zhou, and K. Pahlavan, "WBANs-Spa: An energy efficient relay algorithm for wireless capsule endoscopy," in Proc. IEEE 82nd Veh. Technol. Conf. (VTC-Fall), Boston, MA, USA, Sep. 2015, pp. 1–5.

[4] Chun-I Fan, Yi-Fan Tseng, and Chih-Wen Lin, "Attribute-Based Encryption from Identity-Based Encryption", IACR Cryptography ePrint Archive2017

[5] Javier Herranz, "Attribute-Based Encryption Implies Identity-Based Encryption", IET information security, May.2017

[6] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 332–342, Feb. 2014.

[7] He, D.; Zeadally, S.; Kumar, N.; Lee, J.H. Anonymous Authentication for Wireless Body Area Networks with Provable Security. IEEE Syst. J. 2016, PP, 1–12.

[8] Li, F.; Hong, J. Efficient Certificateless Access Control for Wireless Body Area Networks. IEEE Sens. J. 2016, 16, 5389–5396.

[9] Zhang, A.; Wang, L.; Ye, X.; Lin, X. Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems. IEEE Trans. Inf. Forensics Secur. 2017, 12, 662–675.

[10] H. Xiong, and Z. Qin, "Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1442-1455, 2015.

[11] Chunqiang Hu, Hongjuan Li, Yan Huo, Tao Xiang, , and Xiaofeng Liao, " Secure and Efficient data communication protocol for Wireless Body Area Networks", IEEE. Trans. On Multi-scale Computing, vol.2, no.2, June.2016

[12] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", IEEE Trans. Parallel Distrib. Syst., Vol. 24, no.1, pp. 131-143, Jan. 2013.

[13] Xiong, H., Cost-effective scalable and anonymous certificateless remote authentication protocol. Inf. Forensics Secur. IEEE Trans. 9(12):2327–2339, 2014.

[14] M. Samaneh, A. Mehran, L. Justin, S. David, and J. Abbas, "Wireless body area networks: A survey," IEEE Commun. Surv. Tuts., vol.16, no.3, pp. 1658–1686, Aug. 19, 2014.

[15] Liaojun Pang, Lu Gao, Huixian Li, Yumin Wang, "Anonymous multi-receiver ID-based signcryption scheme", IET information Security, vol.9, no.3, pp.194 – 201, April.2015

[16] Yahong Li, Caifen Wang, Yulei Zhang and Shufen Niu, "Privacy-preserving multi-receiver signcryption scheme for heterogeneous systems", Security and Communication Networks 9(17), October 2016

[17] K.-A. Shim, Y.-R. Lee, and C.-M. Park, "EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks," Ad Hoc Netw., vol. 11, no. 1, pp. 182–189, Jan. 2013.